IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	)	
	)	
CONTENT OF EIGHT FILES	)	Magistrate No. 22-1545
SUBMITTED WITH NCMEC CYBERTIPLINE	)	**[UNDER SEAL]**
REPORT NUMBER 124400321 THAT ARE	)	
CURRENTLY IN THE CUSTODY OF THE	)	
FEDERAL BUREAU OF INVESTIGATION	)	

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Aaron Muscatello, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), assigned to the Pittsburgh, Pennsylvania office. I have been employed as a Special Agent for the FBI since May 2011. As part of my duties, I have investigated violations of federal law, including the online exploitation of children, including violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have participated in the execution of numerous federal and state search warrants which have involved child sexual exploitation and/or child pornography offenses. By virtue of my position, I perform and have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I have personally participated in the execution of numerous federal search warrants involving the search and seizure of computer equipment in cases involving violations of Title 18, United States Code, Sections 2252 and 2252A.

2. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—eight (8) digital files—which is currently in law enforcement possession, and the content of that property described in Attachment B.

3. This Affidavit is submitted in support of an application for a search warrant for the files submitted in connection with a CyberTip (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1), 2252(a)(2), and 2252(a)(4)(B).

4. This Application is part of an investigation initiated by a report known as a "CyberTip" filed with the National Center for Missing and Exploited Children (NCMEC) CyberTipline and involving the suspected possession/trafficking of Child Sexual Abuse Material (CSAM), also referred to herein as "child pornography." As used herein, "CSAM" means visual depictions, including computer images, of a minor (person under the age of 18 years), engaging in "sexually explicit conduct" as defined in 18 U.S.C. § 2256(2)(A), all in violation of 18 U.S.C. § 2252(a). Such conduct includes actual or simulated sexual intercourse of any kind, masturbation, bestiality, sadistic or masochistic behavior, and the lascivious exhibition of the anus, genitals, or pubic area.

5. NCMEC is a private, nonprofit organization that provides services related to preventing the abduction and sexual exploitation of children. NCMEC does not conduct investigations but receives reports of child exploitation and makes those reports available to law enforcement agencies for independent review and investigation.

6. NCMEC also serves as a repository for information about child pornography (also referred to as "child sexual abuse material" (CSAM)). Pursuant to Title 18 U.S.C. Section 2258A, a provider of electronic communication services or remote computing services to the public through a means or facility of interstate commerce, such as the Internet, shall report incidents of apparent violations of child exploitation statues to the NCMEC CyberTipline. To make such a report, a Provider can go to an online portal that NCMEC has set up for the submission of these tips. The Provider then can provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or usernames associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than information such as the incident type and time, the remainder of the information provided by a Provider is provided voluntarily and undertaken at the initiative of the reporting Provider. Such Provider reports may include the suspect image(s) and video(s) that the Provider may or may not have independently viewed. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information provided by the Provider (such as IP addresses). NCMEC then packages the information from the Provider, along with any additional information it has, such as related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

7. This Affidavit is in support of an application for a search warrant upon digital files, the contents of which are the basis for the aforementioned CyberTip.[1] Based upon the information

[1] In or around May 2022, this CyberTip was forwarded to FBI-Pittsburgh. FBI Special Agent Kristen Hummer viewed the CyberTip in its entirety, including the associated 8 files provided by MediaLab/Kik. For the purposes of this Affidavit; however, your Affiant is not relying on any observations made or information received by SA Hummer beyond that which is described in this Affidavit.

contained in this Affidavit, I have reason to believe that on said premises there is now located certain property which is evidence of the above referenced criminal violation(s).

8. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause for the requested search warrant.

RELEVANT STATUTES

9. As noted above, this investigation concerns alleged violations of Title 18, United States Code, Section 2252(a), relating to material involving the sexual exploitation of minors.

a. Title 18, United States Code, Section 2252(a)(1) and (b)(1) prohibits any person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer or mails, any visual depiction if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct; or attempting or conspiring to do so;

b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual

depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or attempting or conspiring to do so.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or attempting or conspiring to do so.

PROBABLE CAUSE

10. On May 10, 2022, MediaLab/Kik reported to NCMEC via CyberTip 124400321, hereinafter referred to as the "**TARGET CYBERTIP**", that the Kik account with the screen/user name "owads2", ESP User ID "owads2_lrl", and registered email address owadsworth10@gmail.com uploaded/shared with another user or group of users seven files of suspected CSAM. MediaLab/Kik indicated that all of these files originated from the same (login) IP address: 73.154.248.91 (Comcast Cable) that resolves to the Monessen area of the Western

District of Pennsylvania (Metro Area-Pittsburgh).[2] Specifically, MediaLab/Kik reported that three (3) videos were sent from this user to another user via private chat message on March 31, 2022 (05:21:00 UTC, 05:29:49 UTC, and 05:29:58 UTC); three (3) videos were sent from this user to another user via private chat message on April 6, 2022 (09:30:47 UTC, 09:31:41 UTC, 09:37:05 UTC).; and one (1) image/jpg was sent from this user to another user via private chat message on April 6, 2022 (09:20:02 UTC). MediaLab/Kik reported the "Incident Type" for the CyberTip as "Child Pornography (possession, manufacture, and distribution)". For each of the seven (7) uploaded files, MediaLab/Kik reported that it had viewed the entire contents of the uploaded file.[3] MediaLab/Kik also provided an additional file to NCMEC stating that the PDF contains "…the most recent basic subscriber data and recent IP address(es), if available, associated to the Kik account: owads2_lrl."

11. CyberTip reports sometimes also include a section wherein NCMEC provides a categorization for uploaded files reported by the electronic service provider; in this instance, MediaLab/Kik. Here, NCMEC noted that the "Automated file categorization is based on NCMEC's review of uploaded files included in the report OR via a 'hash match' of one or more uploaded files to visually similar files that were previously viewed and categorized by NCMEC at the time a PDF of [the] report was generated." Within the CyberTip report, NCMEC indicated that NCMEC automatedly categorized all six videos as "Apparent Child Pornography" and the one image/jpg as "Child Unclothed".

[2] When a Reporting Provider voluntarily reports an IP address for the Suspect, NCMEC Systems will geographically resolve the IP address via a publicly-available online query.

[3] The exact manner of the review of the files associated with this CyberTip by Kik/MediaLab Inc. (i.e., automated, human, or hash match) is unknown to your Affiant.

12. Your Affiant knows through training and experience that a "hash value" is like a digital fingerprint. It is produced when a digital image is analyzed using a complex mathematical algorithm. Every time a particular file or image is processed using the algorithm, the resulting hash value will be the same. If the file or image is altered in any way, even slightly, analysis through the algorithm will produce an entirely different hash value. Thus, a hash value is essentially an identification number for a specific file.

13. Therefore, here, a "hash match" indicates that one or more of the uploaded files reported in the CyberTip are a match to files which NCMEC previously viewed and categorized in its capacity as a repository for information about child sexual exploitation. Based on this, NCMEC listed seven uploaded/shared files in the **TARGET CYBERTIP** with the following categorizations: six (6) were categorized as "Apparent Child Pornography;" and one as "Child Unclothed."

14. Therefore, there is probable cause to believe that the content of the file(s) which MediaLab/Kik reported in connection with the submitted CyberTipline Report 124400321 contains suspected and/or previously-identified CSAM (as well as one file which contains the basic subscriber data and recent IP addresses associated with the MediaLab/Kik account owads2_lrl.)

CONCLUSION

15. The evidence believed to be located within the digital files provided as part of the **TARGET CYBERTIP** further described in Attachment A, which is incorporated by reference as if set forth fully herein, is listed in Attachment B of this Affidavit, which is incorporated by reference as if fully set forth herein, and is believed to consist of at least seven (7) files depicting apparent child pornography and an unclothed child, and one file containing basic subscriber information/IP addresses associated with the Kik account suspected of uploading/sharing the

electronic files. The material is currently in the possession of FBI Pittsburgh, Mon Valley Resident Agency, 17 Arentzen Boulevard, Charleroi, PA 15022. Your Affiant requests authority to search for and seize such material.

16. Because the material is currently in the possession of the FBI, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Respectfully submitted,

/s/ Aaron Muscatello
Aaron Muscatello
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 28th day of November, 2022.

_____
HONORABLE MAUREEN P. KELLY
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The digital files provided by MediaLab/Kik to the National Center for Missing and Exploited Children (NCMEC) and reported by NCMEC to law enforcement via CyberTipline Report 124400321, presently in the possession of FBI Pittsburgh, Mon Valley Resident Agency, 17 Arentzen Boulevard, Charleroi, PA 15022.

ATTACHMENT B

Description of items to be seized

For the digital files described in Attachment A:

1. Any image or video depicting what appears to be any person under the age of 18 engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2)(A), or the contents of which otherwise constitute evidence of the commission of, contraband, or the fruits of violations of Title 18, United States Code, Section 2252(a).
2. Subscriber data and Internet Protocol (IP) address(es) associated to the Kik account: owads2_lrl.